UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/025,572 | 12/26/2001 | Lee Codel Lawson Tarbotton | 01.134.01 | 8371 |

7590 10/05/2005

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

| EXAMINER | |
|---|---|
| MILUTINOVIC, CHARLES | |
| **ART UNIT** | **PAPER NUMBER** |
| 2136 | |

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/025,572 | TARBOTTON ET AL. | |
| | Examiner | Art Unit | |
| | Charles Milutinovic | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *12/26/2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/5/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is in response to application 10/025572 received on Dec. 26, 2001.

2. The IDS of June 5, 2002 has been received and considered.

3. Claims 1-24 are pending.

### *Claim Rejections - 35 USC § 112*

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 18-23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 18-24 recites the limitation "computer program product." There is insufficient antecedent basis for this limitation in the claim.

### *Claim Rejections - 35 USC § 103*

6. Claims 1-3, 6, 8, 9-11, 14, 16, 17-19, 22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg (US Patent 6,021,510) in view of Kim (The Design and Implementation of Tripwire: A File System Integrity Checker), Polk et al. (A Guide to the Selection of Anti-Virus Tools and Techniques), and Jones (Building an E-Mail Virus Detection System for Your Network).

7. In regards to claim 1, Nachenberg discloses an anti-virus acceleration system, which teaches:

- Malware scanning system and methods operable to scan data stored within a storage location addressed by an operating system to identify any data stored within said storage location that contain Malware [Fig. 3, 22]

- Identification system and methods operable if no data containing malware are found in said storage location, to identify said storage location as a clean storage location [Fig. 3; 34, 35]
- When subsequently reading data [Fig. 3, 21, "no"] determining methods operable to determine whether or not said computer file is stored within a clean storage location [36, 37; 25,26]
- If said data is stored within a clean storage location, then permitting reading of said data without further malware scanning [Fig. 3, 39]
- If said data is stored within a clean storage location, then malware scanning of the entire file [27]

What Nachenberg does not teach is that the "data" referenced above is a file or the method is embodied in a computer code product.

Kim et al. teach Tripwire, a security utility that "monitor[s] a designated set of files and directories for any changes ... [to] notify system administrators of corrupted or altered files..." [Kim et al., Abstract, Paragraph 2] Specifically, this teaches that it would be useful to watch for changes to data at the file system level as well as the physical level.

It would have been obvious for one of ordinary skill in the art to take the invention of Nachenberg, and to have the option to monitor at the file system level instead of the physical layer i.e. sectors. The motivations are many, the first being that in the art of system administration the use of command line virus scanners to target items of interest is well known, for example in Jones the use of a virus scanner to target incoming mail messages [Jones, P. 4 Paragraph 2-Paragraph 3]. The files reported modified by a utility emulating tripwire's functionality would certainly qualify as an item of interest, and would allow reports on files and directories which are extremely useful to an administrator, instead of raw sectors which are not. Another motivation comes from Polk et al., which teaches many different classes

of virus detection programs (tripwire being Checksum/Generic Monitor; Nachenberg being Scanner/Checksum), but stating, "the most complete protection will be obtained by combining tools which perform in radically different fashion and protect against different classes of viruses." [Polk et al., 5.1.1, Combining Detection Tools], which in our specific combination would involve the virus scanner of Nachenberg et al. to target the files a utility such as tripwire targets as suspicious i.e. have been modified in addition to its normal duties.

The combined system of Nachenberg and Kim et al. still do not teach that their methods should be executed by computer code.

The invention of Nachenberg does state that the "antivirus scan module [3] can be a conventional antivirus product such as Norton Antivirus (NAV)," [Nachenberg, Col. 3 Line 14] and it is well known in the art that NAV is implemented using computer code. Also, tripwire is written "in the standard K&R C programming language" [Kim et al, Pg. 23 Col. 2 Line 2]. It would have been obvious to one of ordinary skill in the art to combine two inventions both using computer code by using selected pieces of computer code from each in additional to additional "glue" code, hence implementing the methods discussed in Nachenberg and Kim et al. as a computer program product using code.

8. In regards to claim 9, in the rejection of claim 1 we provided reasons why the methods given by Nachernberg et al. were best implemented as computer code. The methods themselves read upon this claim.

9. In regards to claim 17, a computer program product was taught that covers the claim language of this claim. It would have been obvious for someone of ordinary skill in the art, who wished to actually use this computer program product, to install it on a computer and hence create an apparatus to carry out the functions of the computer program product.

10. In regards to claims 2, 10, and 18, "wherein said malware scanning of all computer files stored within a storage location is performed upon a set of user specified storage locations from within all

storage locations accessible to a user," Kim et al. state "The configuration file for Tripwire, tw.config, contains a list of entries, enumerating the set of directory (or files) to be monitored for changes, additions, or deletions." [Kim et al., P. 24 "Configurability and flexibility," Paragraph 3]

11. In regards to claims 3, 11, and 19, "wherein said malware scanning of all computer files stored within a storage location is performed as a background task," in the combined invention of Nachenberg et al. discussed above the trigger for the scan of a clean location is that a file has changed, which then triggers the execution of the scanner. The file change is not necessarily user generated, and the execution of the scanner requires no user intervention, hence it can be considered a background task.

12. In regards to claim 6, 14, and 22, "wherein said malware scanning code uses malware definition data to identify malware and, upon updating of said malware definition data to give updated malware data, said storage location is no longer identified as a clean storage area until it has been malware scanned using said updated malware definition data and no computer files containing malware are found in said storage locations," Nachenberg teaches that one of the conditions of "examined an initial time" is that "A virus definition within antivirus scan module [3] has been changed" [Nachenberg et al., Col. 3 Lines 35-36], and hence if the malware definition data changes then all the files of the clean storage area would be rescanned as per [Fig. 3, 21] to maintain the cleanliness of the storage area.

13. In regards to claim 8, 16, and 24, Nachenberg teaches that the "antivirus scan module [3] can be a conventional antivirus product such as Norton Antivirus (NAV)." [Nachenberg, Col. 3 Line 14] It is well known in the art that NAV is able to detect many categories of malware, most notably, as the name implies, computer viruses.

14. Claims 4, 12, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg et al. as applied to claims 3, 11, and 19 above, and further in view of Cohen (Current Best Practice Against Computer Virus).

In the system of Nachenberg et al. discusses in claims 4, 12, and 20 we are using the default NAV command line scanner, i.e. the on-demand vs. the on-access scan. It is well known in the art that on-access scanners are built to be faster then on-demand scanners as a matter of course, since a slow on-demand scanner would compromise the user's experience. In Cohen's article he explicitly gives credence to this idea from a practical standpoint as well, stating "There are a number of variations on scanners, most notably the so-called 'monitor,' which is a variation on the 'integrity shell' technique ... which dramatically reduces the costs associated with detecting known viruses." [Cohen, Pg. 262 Col. 2 Paragraph 2].

15. Claims 5, 13, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg et al. as applied to claims 1, 9, and 17 above, and further in view of Symantec.com (Norton AntiVirus 2001 for Windows 2000/NT/Me/98/95).

It is well known in the art that any newly created file should be scanned for viruses. Symantec.com reinforces this principal, stating that it "scans files you download from the web, as well as attachments you get through email." [Paragraph 1, lines 5-7]

16. Claims 7, 15, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg et al. as applied to claims 6, 14, and 22 above, and further in view of Green et al. (Vesseling Bontchev's paper 'Vircing The Irvircible' [long] (pc)) and Probert (Timid).

Nachenberg et al. teach all the limitations of claims 6, 14, and 22. What they do not teach is that "when the storage area is being malware scanned with said updated malware definition data, computer files written to said storage location after said storage location after said storage location was previously identified as a clean storage location are malware scanned before computer files that are unaltered since said storage location was previously identified as a clean storage location."

In Green et al.'s Usenet thread, specifically in the reply by Bill Lambdin it is taught "Viruses can use Dos call 57h to check the time and date stamps of files before infection, and if the files are less then 1 day, one week, one month, etc., ignore the bait file..." [Reply 3 dated Sep 6, 1996; 3.h]

In Probert, we are given the source code to a virus in the TIMID family. One specific advantage that this virus has that other viruses' in the TIMID family do not is "The virus also save target file attributes and restores them on exit so that date & time stamps aren't altered ..." [Paragraph 1, lines 8-11]

It would have been obvious for one of ordinary skill in the art to take the invention of Nachenberg et al., and to perform the scan of files added to the clean location after said storage location was identified as a clean storage location first after a definition update. It is known in the art of anti-virus that computer users loath the time on-demand scans take, often canceling the scan before it is complete, and hence it would make sense to configure an engine to scan the most vulnerable items first. Green et al. teaches that certain classes of viruses target only newer files, and hence it would make sense to scan these files first as they are vulnerable to more viruses. In addition, Probert strongly suggests that this idea, the targeting of newer files first as a weakness in viruses, was known in the art as one specific feature of the virus he teaches is to keep the timestamps intact upon infection.

### *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles Milutinovic whose telephone number is (571)272-2668. The examiner can normally be reached on M-F 8:30-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

***